

ISCEs of MCA projects as they go through the design process under ACSIM control and USACE execution. As subsequent design reviews (from the initial reviews through the final reviews) are completed, USAISEC-FDEO updates the ISCE and gives copies to USACE, the MACOM, and the DOIM involved with each particular project.

(b) USAISEC-FDEO routinely reviews and updates the ISCEs of MCA projects as they progress through the design process under ACSIM control and USACE execution. As subsequent design reviews (from the parametric design phase through the final engineering design reviews) are completed, USAISEC-FDEO updates the ISCE and gives copies to USACE, the MACOM and the DOIM involved with each particular project.

(c) USAISEC-FDEO participates as a member of the planning charrette as the technical advisor to the DOIM, RCIO, and MACOM. Coordinates with the installation DOIM to determine the telecommunication requirements for the project.

(d) USAISEC-FDEO integrates the ISCE into the project's overall requirements and tracks subsequent ISCE throughout the project.(4).

Chapter 8

Army Public Web Site Management

8-1. Web site planning and sponsorship

a. *Target audience.* Web sites should be made publicly accessible on the Internet only when the target audience includes the public at large. Information that is for Army personnel only should be moved to AKO or other approved private Web site. Private (intranet) Web sites must migrate to AKO per AR 25-1, paragraph 3-9.

b. *Accurate information.* Users of Army public Web sites must be assured access to accurate official information, regardless of whether the site is linked only to other Government Web sites or also to private sector Web sites.

c. *Web Site purpose and plan.* Each Army organization that establishes a public Web site (or Web presence) must have a clearly defined purpose and Web site plan supporting the organization's mission. The plan should be approved by the organization's parent command or organization. The Web site plan addresses at least—

- (1) Web site registration.
- (2) Identification of Webmaster contact information.
- (3) Procedures that explain administration of the Web site on—
 - (a) Posting of information.
 - (b) Reviewing the site for content and format.
- (4) Contingency and continuity of operations.

(a) The plan should state what the sponsor will do with the Web site(s) during disasters or emergencies, including important information and services to be provided to the public.

(b) Web site plans will be documented in the organization's continuity of operations plans.

d. *Domains.* New Army public Web sites are established in the army.mil domain to show that they are official sources of Army information. This applies to all Web sites. Organizations using non-.mil domains should execute plans to transition Web sites to the army.mil domain in order to comply with Federal Web site policy. Exceptions to the use of the army.mil domain should be submitted to the Army CIO/G-6, SAIS-GKP.

e. *Web site listings on the Army HomePage.* The Army HomePage (<http://www.army.mil/>) provides public Web site locator information for the Army's units and installations (Army A-Z). Organizations and installations with public Web sites will ensure that their sites are posted on the page. Fill in the Web maintainer and sponsor contact information for the Web site and the URL in the contact us link at the bottom of the page.

f. *Registration approval.* Registration for army.mil domain requests is achieved through the following processes:

(1) Army Internet registration is a part of the mission of the CONUS Theater Network Operations and Security Center (CONUS-TNOSC), <http://www.conus-tnosc.army.mil>. CONUS-TNOSC is part of NETCOM/9th ASC. NETCOM supports Army installations needing to apply for Internet protocol addresses via the NIPRNET and SIPRNET.

(2) DOIM or others with registration duties select the Internet registration option on the TNOSC Web site and inform the Army community they support. These online instructions lead the user to downloadable templates for providing the required information. When the template is completed, users send it directly to domain-request@aims7.army.mil.

g. *Web records administration.* Web records must be managed per OMB Circular A-130 and guidance from the National Archives and Records Administration (see 36 CFR 1220-1238 and www.archives.gov/records_management/index.html).

h. *Web masters/maintainers.* Army organizations assign a Web master for each public Web site they sponsor. The Web master/maintainer has technical control over the registration process, managing the site's content, and ensuring the site conforms to Army Web site requirements.

i. *Sponsorship display.* Army public Web sites must clearly display "U.S. Army" on every page along with the organization's official name and include a statement that the Web site contains official Government information. Home

pages and second tier pages include a page title, as part of the metadata, with the organization's name identified as the site sponsor.

j. Labeling. Accessible information will be labeled to indicate the following where appropriate:

- (1) Draft policies, regulations, and other predecisional information are not posted on public Web sites.
- (2) Copyrighted information for which releases from the copyright owner have not been obtained.

k. Web site linking. Army public Web sites will follow these requirements when linking to other Web sites:

- (1) Use only text or hyperlink text to direct users to non-Army software download sites.
- (2) Post a link to a "process for linking to non-Army sites" and include guidelines for selecting and maintaining external links. The decision to use a link to an external source must exhibit sound public policy and support the Army's mission. Organizations linking procedures must explain why some links are chosen and others are not. The links must be chosen fairly and in the best interest of the public (see AR 25-1, para 6-4n).

(3) The linking policy found on FirstGov.gov is suggested as an example for developing Army public Web site linking policies. Hyperlinks to Web resources other than official U.S. Government Web resources are permitted only if the organization's mission requires them (see AR 25-1, para 6-4n for policy on linking to non-Government Web sites).

l. Date posted data. Army public Web sites will clearly state the date the content was posted or updated for every Web page, indicating to visitors that the content is current and reliable. Web masters/maintainers should include a statement such as, "Last updated on ___" or a date stamp to each page altered or reviewed.

8-2. Content propriety and quality

a. Information of value. Army public Web sites should only post information of value to their visitors. These visitors include users from Army organizations, other Government agencies, academies, the private sector, and citizens with an interest in the missions performed.

b. Content limitations. Army public Web sites content will comply with the following content limitations:

(1) Abbreviations should not be used on the front page but may be used on sub-pages if the words are spelled out first.

(2) The .mil Web sites may not be directly linked to or refer to Web sites created or operated by a political campaign or committee.

(3) The Army Web content owner ensures that information submitted for posting to an Army public Web site is current, timely, and cleared for applicable release by the public affairs officer or other designated official to ensure compliance with AR 25-1, paragraph 6-4n, and at appendix C.

c. Content organization. Information should be organized by subject/topic, by audience group, by geographic location, or by any combination of these factors, based on an analysis of the visitor's needs.

d. Content focus. The content should be the main focus for the target audience and serve as a general index to all major options available on the Web site. Home pages will minimize extraneous content to allow visitors to get to the content it needs and wants most.

e. Exclusive information. Web sites should not contain information that is meant exclusively for organization employees and is of little or no use to the private sector except in emergency or other exceptional situations. Information for an organization's exclusive use should be contained in AKO or other approved intranet site.

f. Public Web site content. Web masters/maintainers should provide the following content in each Army public Web site:

(1) A link to a page entitled "Contact Us" or "Contact (Organization Name)" from the home page and every major point of entry. Contact information will be generic and will include—

(a) Organization's street address, including addresses for any regional or local offices.

(b) Office phone number(s), including numbers for any regional or local offices.

(c) Means to communicate by electronic mail (for example, organizational e-mail address or Web-based contact form (for example xxxwebmaster@us.army.mil)).

(d) The organization's policy and procedures for responding to e-mail inquiries, including whether the organization will answer inquiries and the expected response time.

(e) Contact information, as required by information quality guidelines.

(f) Contact information (office names/titles/phone numbers) for small businesses as required by the Paperwork Reduction Act.

(g) Means to request information through FOIA. Make FOIA information requests by e-mailing FOIA@rmda.belvoir.army.mil.

(2) Main entry point Web sites (for example, Army Home Page, Army Reserves, Army National Guard, MACOMs), which should include a link to a page entitled "About Us" or "About (Organization Name)" from the home page. Organizational information will include at least all of the following:

(a) A description of the organization's mission, including its statutory authority.

(b) A strategic plan, vision, or set of principles.

(c) An organizational structure, including basic information about parent and/or subsidiary organizations and regional and field offices, as appropriate.

(d) Contact information, which may include e-mail addresses, phone number, office, name, or position.

(e) Information about jobs at the organization. The preferred method is to link to Civilian Personnel On Line (<http://acpol.army.mil/employment/index.htm>).

(f) A link to a site map or subject index that gives an overview of the major content categories on the site. At a minimum, a link to the site map or subject index will be provided from the home page.

(g) A link to a “Common Questions” or “Frequently Asked Questions” Web page providing basic answers to questions the organization receives most often.

(h) Easy access to existing online citizen services and forms that are applicable to the general public. These items should be displayed as prominently as possible, and based on an analysis of customer needs.

(i) Information about professional opportunities in organizations.

(j) Links to a portal for the most frequently requested publication(s).

(k) Web site policies and important notices. Organizations will post (or link to) a page entitled “important notices” at the footer of every Web page. The important notices page describes the principle policies and other important notices that govern the Web site, especially those mandated by law. At a minimum, this page will include—

1. Privacy policy. Include in this policy a statement that the site does not use “persistent” cookies or any other automated means to track the activity of users over time and across Web sites.

2. Security policy.

3. How to request information under FOIA.

4. Accessibility policy.

5. Information quality guidelines.

g. *Assessing the user’s satisfaction.* Army public Web site sponsors should conduct an annual assessment of user satisfaction with the Web site, including usability to identify needed improvements.

h. *Army installation newspapers.* Army installation newspapers are authorized and established according to AR 360–1. Though generally public domain, these newspapers are part of the Army internal information program. While publishing installation or organization newspapers constitutes public release of information, the distribution is limited. Publishing on an unlimited access Web site represents global release. Some information appropriate for installation newspapers is not appropriate for public Web sites. Army organizations may reproduce the content of installation newspapers for the Web if that content meets the restrictions provided in AR 25–1, paragraph 6–4n. These restrictions include prohibitions against posting names, locations, and specific personal identifying information about employees and military personnel and their family members. Advertisements appearing in private sector newspapers should not be posted on Web sites.

i. *Commercial use of communications systems.* Use of communications systems for commercial purposes in support of for-profit activities or for personal financial gain is prohibited (see AR 25–1, para 6–1f).

8–3. Usability criteria

The usability guidelines contained at <http://www.usability.gov> may be a valuable tool for Web site designers.

a. *Accessibility.* Army public Web sites must be accessible to all citizens (see to AR 25–1, para 6–4 and para 7–5, above).

b. *Public Web site requirements.* Public Web sites should be developed according to the following guidelines:

(1) Web master/maintainers will ensure that pages are designed, developed, and tested for multiple browsers, operating systems, connection speeds, and screen resolutions, based on an analysis of an organization’s Web site visitors. Army public Web sites will, to the maximum extent feasible, minimize page download times for their visitors.

(2) Web sites should be compliant with Section 508, designed to make online information and services fully available to citizens with disabilities. The important notices page described in paragraph 8–2e(8) must include a link to an accessibility policy that describes compliance with the Act.

(3) Information should be presented using plain language which considers the knowledge and literacy level of the typical visitor. The text must be gender neutral and be accessible to persons who, as a result of national origin, are limited in their English proficiency. Understandable language and content criteria are included in any customer satisfaction survey.

(4) File formats used will be based on operational needs of the organization and the needs of the customers. Organizations will provide information in a format that does not require the public to use plug-in or additional software, if it imposes a burden. When a Web page requires an applet, plug-in or other application in order to interpret the page content, the page should provide a link to a plug-in or applet. When choosing the file format, the organization will consider—

(a) The intended use of the material by the target audience.

(b) The accessibility of the format to the target audience.

(c) The level of effort required to convert the material to the format.

(5) Organization Web sites that link to documents requiring downloading will provide sufficient contextual information so visitors have a reasonable understanding of what to expect when they view the material.

(6) Proprietary formats are only used when the audience is known to have easy access to software able to read the format. Raw data files provide the greatest flexibility for the public and are preferred over proprietary formats requiring specific commercial software. Consistent navigation schemes between and within all Army public Web sites will be used.

(7) Visitors are more likely to get what they need from a site if changing navigation doesn't confuse them. Standard navigation criteria is provided as follows:

(a) Common items appearing on most Web pages will, if possible, be in the same location on each page and have the same appearance and wording. A navigation item that is shared by a group of pages (such as a set of pages on a single topic, or for a division of the organization) will also have the same location, appearance, and wording on each page.

(b) Navigation items of the same type will look and behave like each other. For example, if a set of pages on one topic has subtopic links in the left navigation bar, pages on other topics will have subtopic links in the left navigation bar that are similar.

(c) If a set of Web pages requires specialized navigation, that navigation is applied to the largest possible logical grouping (such as a topic, an audience, or a complete organizational unit). The specialized navigation will be similar in appearance and behavior to your overall navigation scheme.

(8) Web masters/maintainers should include either a search box or a link to a search page from every page of the Web site. The search box or link will be entitled "search." Place subject and keywords in source code to aid content searches. Focused searches may be given to search within sets of information, databases, or applications. Web sites that are narrow in scope or under 200 pages may substitute a site map or A to Z index rather than implement a search engine. Army public Web sites will have the following minimum service level standards:

(a) What is the extent of search engine crawling and indexing? What types of documents are crawled and indexed? How often are they crawled and indexed?

(b) What are the best ways to search your documents or collections? Will visitors enter phrases or keywords? What other hints can you give visitors?

(c) What is the expected search response time? For example, 95 percent of searches get a result set returned within 5 seconds.

(d) How can customers use the search engine for more precise searching and browsing (that is, minimum chaff) or for recall (that is, maximum wheat)? For example, if searching for a specific marketing report, include the country name, the year, and the type of report, for example, strategic planning.

(9) Include the following five meta tags on all home pages and major entry points:

(a) Page title.

(b) Description.

(c) Creator/sponsor (in most cases, the organizational name).

(d) Date created.

(e) Date reviewed.

(10) Web site visitors will be informed about major proposed and implemented changes to the Web site. Web-masters/maintainers should place a notice on the home page informing visitors about the change, insert redirect notices when page destinations are changed, and clarify changes on the Help page.

8-4. Training and compliance

a. Sponsor functions. Army public Web site sponsoring organizations must ensure that Web site development, maintenance, and operations staff understand applicable requirements specified herein. The sponsor ensures that the public affairs officer or other appointed official reviews and clears the Web content during the establishment of the site and conducts quarterly reviews of updated content. (AR 25-1, para 6-4*n*, and appendix C-4 contain Army policy on Web site prohibitions for content pertaining to operational security, privacy, sensitive information, pre-decisional information, information exempt from Freedom of Information Act, copyrighted information, commercial sponsorship and advertising, and others.)

b. Training. All individuals appointed to be Web masters/maintainers, reviewers, and content managers must complete training and certification, as necessary, equal to the duties assigned to them. Web-based training is available at AKO (<https://iatraining.us.army.mil>). This course is mandatory for all webmasters/maintainers.

8-5. Consistent and nonredundant information

a. Redundancy. Content and services provided via Army public Web sites should not be redundant or in conflict with each other. The following requirements will be implemented by all Army public Web sites so that this is achieved.

b. Links to information. Web sites should link to existing Government-wide portal or specialized sites when applicable, rather than recreating these resources themselves.

(1) Before creating new information, the organization determines if that same or similar information already exists within their organization or on another Army, DOD, or Federal Web site.

(2) When an organization Web site provides information or services for which there is a corresponding Government-wide portal or specialized site, the organization will link to the Government-wide portal or site from its pages on that topic.

(3) When a Government-wide portal or specialized Web site is available on a subject that the public would expect to find on an organization's site, but the organization does not provide that information, the organization will link to the Government-wide portal or site in a logical and useful location.

(4) Organizations should not link to Government-wide portals or specialized information unless they are related to the organization's mission or function or might be seen as being related. Links that are not related to a Web site's content can be deceptive and confusing.

(5) Organizations should not re-post documents that other organizations originated. Instead, they should provide links to those documents that are posted on the Web sites of the content owners. Organizations should consult with each other to find ways to share or coordinate content and to mitigate duplication.

(6) As with all links, organizations will review links to the content on other organization Web sites or to portals and specialized Web sites regularly to ensure they are current and accurate.

c. Home page link. To improve Web site utility, each Web page links back to the Web site home page. If an organization uses a graphical link, it contains text indicating that it links to the home page. Headquarters staff elements and major commands should provide a link back to the Army home page (www.army.mil). Subordinate elements of a major command should provide links back to the respective major command and the Army Home Page.

d. Firstgov.gov link. Major organizational home pages (Army Home Page, MACOM, HQDA staff element) should link to the FirstGov.gov home page (www.firstgov.gov) with the entry: "FirstGov: U.S. Government Web Portal."

8-6. Federal law, regulation, and policy compliance

a. Army public Web sites comply with applicable Federal law, regulations, and policies.

b. Refer to AR 25-1, paragraphs 6-1 and 6-4n, for official and authorized use of Government communications and prohibited usage and for Army Web policy, respectively, and appendix C-4 for Web policy management controls. Refer to at www.defenselink.mil/webmasters for DOD policy and guidance and www.firstgov.gov/webcontent/index.shtml for Federal policy and guidance.

8-7. Director of information management Web site administration

a. DOIM functions. DOIMs are required to—

(1) Develop and disseminate local procedures and controls for security and access for installation-hosted Web sites (see AR 25-1 and AR 25-2 for Army Web policy).

(2) Control all Internet connections, to include military-controlled access paths and alternate Internet access paths, such as Internet service providers.

(3) Ensure all traffic destined for other military sites (within the ".mil" domain) is only routed through military controlled networks (that is, traffic destined for military sites will not be routed through an ISP and traffic from an ISP will not be routed through the receiving base network to other military networks).

(4) Ensure "army.mil" network domains are not advertised through ISP connections and are protected by an Army reverse proxy server.

(5) Ensure access to the Internet is secured to acceptable risk levels.

(6) Audit the network continually to locate unauthorized public access Web servers and unapproved limited-access Web servers. For unauthorized public access Web servers, the DOIM or designate contacts the supervising Web site owner moves data to the NOSC/NOSC-D/NCC/NCC-D server, and takes action to disconnect the unauthorized public-access server from the network. Take appropriate action to ensure the network and the information are protected.

b. Procedures. DOIMs or other IT providers should establish procedures for their customers on governing the administration of the Web server environment. As a minimum, procedures should address—

(1) Operation of the Web server environment.

(2) Security of the Web server environment.

(3) Maintenance of access and security control features and ensuring that warning and consent to monitoring notices are installed as appropriate.

(4) Process to ensure DAA approval is re-issued if any Web server environment configuration is changed.

(5) Process to ensure all links from pages under DOIM control is appropriate and valid.

(6) Procedures for content providers and page maintainers to post on the Web server.

(7) Granting and monitoring write-access privileges.

(8) Maintaining and evaluating audit control logs.

(9) Gathering and analyzing performance data.

(10) Developing, coordinating, publishing, maintaining, and testing support plans for contingency and service restoration.

(11) Coordinating mirror or replication sites with other system administrators, as required.

(12) Implementation of security and access controls requested by content providers and page maintainers as required.

(13) Access list for administration/maintenance.

(14) A feedback mechanism for users' comments in accordance with the Paperwork Reduction Act of 1995..

(15) Compliance with federal policies on privacy and data collection on Web sites. Privacy (and security) policies should be clearly posted and easily accessed on the front page of the Web site.

(16) Cooperation with AWRAC for notification of a violation. DOIMs will ensure that Web sites links are disconnected until corrections have been completed (see AR 25-1, para 6-4*n*).

(17) Compliance with Section 508 provisions to make information on Web sites accessible to employees and the public. See Federal accessibility standards at <http://www.section508.gov/index.html> for the latest information. At a minimum these include—

(a) A text equivalent for every nontext element will be provided (for example, via "alt" (alternative text attribute), "longdesc" (long description tag), or in element content.

(b) Web pages designed so that all information conveyed with color is also available without color, for example from context or markup.

(c) Pages designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.

(d) Documents organized so they are readable without requiring an associated style sheet.

(e) Web pages updated for equivalents for dynamic content whenever the dynamic content changes.

(f) Redundant text links instead of server-side image maps except where the regions cannot be defined with an available geometric shape.

(g) Client-side image maps whenever possible in place of server-side image maps.

(h) Row and column headers identified for data tables.

(i) Markup to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.

(j) Frames titled with text that facilitates frame identification and navigation.

(k) A link to a plug-in or applet providing equivalent information on an alternative accessible page, when a Web page requiring that an applet, plug-in, or other application be present on the client system to interpret page content the page.

(l) A text-only page, with equivalent information of functionality, to make a Web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page will be updated whenever the primary page changes.

(m) A method that permits users to skip repetitive navigation links.

(n) When pages utilize scripting languages to display content, or to create interface elements, script-provided information identified with functional text that can be read by assistive technology.

(o) When electronic forms are meant to be completed online, a form to allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.

(p) When a timed response is required, the user will be alerted and given sufficient time to indicate more time is required.

c. *Army Web risk assessment cell (AWRAC)*. The AWRAC reviews the content Army publicly accessible Web sites (.mil and all other domains used for communicating official information) to ensure they are compliant with DOD and Army policies and best practices. The AWRAC—

(1) Conducts random sampling of Web sites to identify security concerns or review Web site concerns provided by the Joint Web Risk Assessment Cell (JWRAC) or Army leadership.

(2) Ensures inappropriate security and personal information is removed from publicly accessible Web sites.

(3) Ensures that Army sites are compliant with other Federal, DOD, and Army Web site administration policies (for example, GILS registration).

(4) Notifies the Web site owner with operational authority and the Information Assurance Program Managers of respective command/activity of violations and suspense dates for reporting corrective action.

(5) As required, reports deficiencies and corrections to the Army CIO/G-6 and JWRAC.

d. *System security considerations*.

(1) Each organization will establish information system security certification and accreditation procedures in accordance with DODI 5200.40.

(2) Operators of Web server environments should be trained in technical information security best practices, or should have immediate access to appropriately trained individuals. Security maintenance and administration should be

considered an essential element of Web site operation and maintenance at all times. It is essential that Web server environment be implemented and maintained by certified personnel. Day-to-day maintenance of the hardware and software, including security patches and configurations, is essential to the system security of Web server environments. See also National Institute of Standards and Technology (NIST) Special Publication 800-44.

(3) A formal risk assessment should be conducted at each organization operating a Web site to determine the appropriate risk management approach based on the value of the information; the threat to the Web server environment and the information contained thereon; the vulnerability of the Web server environment and the information contained thereon; and the countermeasures employed by the Web server environment. A security policy should be written for each Web server environment or multiple sites furnishing similar data on the same system infrastructure or architecture based on the results of the risk assessment.

(4) Web servers that are externally accessed should be isolated from the internal network of the sponsoring organization. The isolation may be physical, or it may be implemented by technical means such as an approved firewall. The server software will be compliant with Federal Information Systems (FIPS) 140-2, with all security patches properly installed. Approved security protocols will be used for all Web servers. Additional security measures should also be employed consistent with the risk management approach and security policy of the individual Web site. Examples of additional measures to be considered include—

- (a) Disabling IP forwarding, avoid dual-homed server.
- (b) Employing least privilege.
- (c) Limiting functionality of Web server implementation.
- (d) Employ tools to check configuration of host.
- (e) Enabling and regularly examining event logs, to include—

1. Back-up methodology as part of the Web site architecture. Information should be replicated to the backup environment to ensure that the information will not be lost in the event that the Web server environment is corrupted, damaged, destroyed, or otherwise compromised.

2. ID and password protection. The internet is an unsecured network where compromise of user ID and password can occur during open transmission. IDs and passwords should not be transmitted without encryption. Secure protocols (for example, secure sockets layer protocol) provide a transmission level of encryption between the client and server machines (see AR 25-2).

Chapter 9

Software and Hardware Asset Management

9-1. Acquisition

The best method of acquiring software and hardware is through solutions based on COTS or a reuse of Government-off-the-shelf products that comply with Army specified standards. The suitability of products for satisfying operational requirements must be evaluated before initiating a development effort. This evaluation is performed by local installation DOIMs or the program executive office (PEO) associated with this acquisition. The evaluation should also determine integration risks associated with the COTS products.

a. *Enterprise Software Initiative (ESI)*. It is DOD policy that before purchasing any COTS software product, the Army acquiring official determines if it is managed under the ESI. Enterprise software agreements (ESAs) negotiated with specific software publishers or their agents offer the best prices and terms. OSD has authorized each service to manage various categories of software applications (for example, database, desktop, graphics, operating systems, and servers) for all of DOD. The Army acquiring official coordinates the acquisition with the designated DOD ESA product manager for that product prior to entering any agreement with any COTS vendors.

(1) If an existing ESA does not contain desired terms or prices, the acquiring official must notify the ESA product manager and allow them to improve the existing ESA before executing other agreements. The Army Small Computer Program (ASCP) is the Army's software product manager. As the designated software product manager, ASCP is responsible for managing the Army's ESA products. Army customers must request waivers for commercial software not being acquired from a DOD ESI agreement at the ASCP Web site, <https://ascp.monmouth.army.mil>. The DOD ESI homepage lists all ESI managed software and is located at www.esi.mil.

(2) The Army entered into an enterprise license agreement for word processing, spreadsheet, database, and presentation software products. Details and ordering information are provided on the ASCP Web site. As organizations increasingly turn to COTS application package solutions for requirements that were met before by in-house or contractor software development projects, care must be taken to ensure that the selected COTS solution meets the organization's requirements. The suitability of COTS or Government off-the-shelf applications for meeting operational requirements must be gauged before starting a development effort.

b. *ASCP office*. The ASCP is the primary source for purchase of COTS software, desktops, and notebook computers regardless of dollar value, and for all other IT purchases greater than \$25K. All commercial IT purchases must be